有用性、ロギング、監視、およびメトリック

ロギングの設定

Expresswayはトラブルシューティングと監査を目的としたsyslog処理機能を提供します。イベントログはローテーションローカルログで、送受信されたコール、登録、およびメッセージなどの情報を記録します。

Expressway ロギングオプションを設定するには、**[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。**[ロギング（Logging）]** ページから次のタスクを実行できます。

- イベントログ冗長性の変更を指定して、ローカルに記録されるイベント情報の詳細レベルを変更する
- コールのメディア統計情報ロギングを切り替える
- コール詳細レコードのキャプチャを切り替える
- 認定対応のロギングを切り替える
- 1 つ以上のリモート syslog サーバへのログの公開 アドレスを定義する
- 各リモートsyslogサーバに送信されるイベントをシビラティ（重大度）でフィルタリングする
- システムメトリック収集（収集済み）の構成方法を切り替える

イベントログ冗長性の変更

ローカルイベントログの冗長性を 1～4 の間で設定することで、ローカルログの冗長性をオプションで制御できます。すべてのイベントには、1～4の範囲で関連付けられたレベルがあり、レベル 1 のイベントが最も重要と見なされます。

（注） レベル 3 またはレベル 4 のロギングは通常運用には推奨しません。このような詳細なロギングによって 2 GB のログが早急にローテーションする可能性があります。ただし、トラブルシューティングではこのレベルの詳細を記録する必要がある場合があります。

イベントは、リモートロギングが有効になっているかどうかに関係なく、常にローカルに（イベントログに）記録されます。

次の表に、さまざまなイベントに割り当てられるレベルの概要を示します。

レベル	割り当てられるイベント
1	登録要求やコール試行などの高レベルイベント。人間が簡単に読み取れます。次に例を示します。 • コール試行/接続/切断 • 登録試行/承認/拒否
2	すべてのレベル 1 のイベントに加えて、次のイベントがあります。 送受信されたプロトコル メッセージのログ（SIP、H.323、LDAP など）。H.460.18 キープアライブや H.245 ビデオ高速更新などのノイズの多いメッセージは除きます。
3	すべてのレベル 1 およびレベル 2 のイベントに加えて、次のイベントがあります。 • プロトコルのキープアライブ • コール関連の SIP シグナリング メッセージ
4	最も詳細なレベル：レベル 1、レベル 2、およびレベル 3 のすべてのイベントに加えて、次のイベントがあります。 • ネットワーク レベルの SIP メッセージ

ログレベルを変更すると、Web インターフェイスを通じて表示するイベント ログと、別のリモートログサーバにコピーされる情報の両方に影響します。変更は振り分け的な操作ではなく、変更後にログに記録される情報にのみ影響します。

Expressway はローカルログに次の機能を使用します。（ローカル）機能にマッピングするソフトウェアコンポーネント/ログが強調表示されます。

- 0（kern）
- 3（daemon）
- 16（local0）管理者
- 17（local1）設定
- 18（local2）*Mediastats*
- 19（local3）*Apache* エラー
- 20（local4）*etc/opt/apache2*
- 21（local5）開発者
- 22（local6）ネットワーク

イベントとレベルセクションには、Expressway によってログに記録されるすべてのイベントと、それらがログに記録される詳細レベルの完全なリストがあります。

認定対応のロギング

環境によっては、Expressway のログがセキュリティ認定の要件を満たすようにする必要があります。セキュリティと診断目的のログの間にはトレードオフがあります。認定対応モードでは、コールの問題の正確な原因を判定できない場合があります。

認定対応ロギングの設定方法

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[ロギングオプション（Logging options）]** セクションで、**[認定ロギング（Certification logging）]** モードを次のいずれかに設定します。

認証ロギング モード	説明（Description）
診断	このモードは認証対応ではありませんが、コールの問題の診断には最も役立ちます。
秘密	このモードは認定対応ではありません。
秘密と詳細	このモードも認証対応ですが、Syslog サーバへのセキュアな接続を使用して一部のログ情報を収集できます。これらのログは、診断の意味では特に役立つものではありません。

リモート syslog サーバへのログの公開

syslog は、複数のシステムからのログ メッセージを 1 つの場所に集約するための便利な方法です。これは、クラスタ内のピアの場合に特に推奨します。

- 最大 4 つのリモート syslog サーバにログ メッセージをパブリッシュするように Expressway を設定できます。
- syslog サーバは次の標準プロトコルのいずれかをサポートする必要があります。
  - BSD（RFC 3164 で定義）
  - IETF（RFC 5424 で定義）

リモート syslog サーバの設定

（注）
- **[キーワード別にフィルタリング（Filter by Keywords）]** オプションは、シビラティ（重大度）別にすでにフィルタリングされているメッセージに適用されます。
- 単語のグループ（「「login successful」」など）を含め、最大 5 つのキーワードをカンマで区切って使用できます。
- 最大 256 文字をキーワードに使用できます。
- システムのパフォーマンスへの影響を回避するために、最も関連性の高いキーワードを最初に検索することを推奨します。これにより、syslog サーバに関連するログ メッセージができるだけ早期にプッシュされます。

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動し、このシステムがログメッセージを送信する**リモート syslog サーバ**の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 2 各サーバの [オプション（Options）] ボタンをクリックします。

ステップ 3 使用する**転送**プロトコルと**ポート**を指定します。TLS を使用する場合、syslog サーバに対して証明書失効リスト（CRL）を有効にするオプションが表示されます。

ステップ 4 [メッセージ形式（Message Format）] フィールドで、リモート Syslog メッセージの作成形式を選択します。デフォルトは [レガシー BSD（Legacy BSD）] です。

ステップ 5 **[シビラティ（重大度）別にフィルタリング（Filter by Severity）]** オプションを使用して、送信する詳細レベルを選択します。Expressway は選択したシビラティ（重大度）のメッセージと、より厳しいメッセージすべてを送信します。

ステップ 6 **[キーワード別にフィルタリング（Filter by Keywords）]** オプションは、特定のキーワードを含むメッセージを送信する場合に使用します。

ステップ 7 [保存（Save）] をクリックします。

使用される一般的な値

次の表に、ロギングサーバとネットワーク設定に最適な形式を選択する上で役立つ情報と、一般的な値を示します。

表 *1 : Syslog* のメッセージ形式

メッセージ形式	トランスポートプロトコル	提案されたポート	RFC
レガシー *BSD* 形式	UDP	514	BSD 形式。RFC 3164 を参照
IETF syslog format	UDP	514	IETF 形式。RFC 5424 を参照
TLS 接続を使用した *IETF syslog*	TLS	6514	IETF 形式。RFC 5424 を参照

（注）

- UDP プロトコルはステートレスです。ご使用の環境で syslog メッセージの信頼性が非常に重要である場合は、別のトランスポート プロトコルを使用する必要があります。
- Expressway と syslog サーバ間にファイアウォールがある場合、適切なポートを開いてメッセージを通過させる必要があります。
- TLS トランスポートを選択した場合は、Expressway は Syslog サーバの証明書を信頼しなければなりません。必要に応じて、Syslog サーバの CA 証明書をローカル信頼ストアにアップロードします。
- TLS の使用時は CRL チェックはデフォルトで無効になっています。CRL を有効にするには、**[CRL チェック（CRL checking）]** を *[オン（On）]* に設定し、関連する証明書失効リスト（CRL）がロードされるようにします。

  詳細については、「セキュリティの基礎」を参照してください。
- リモート サーバを別の Expressway として使用することはできません。
- Expressway は他のシステムのリモート ログ サーバとして機能できません。
- Expressway はリモート ロギングに次の機能を使用します。（ローカル）機能にマッピングするソフトウェアコンポーネント/ログが強調表示されます。
  - 0（kern）
  - 3（daemon）
  - 16（local0）管理者
  - 17（local1）設定
  - 18（local2）*Mediastats*
  - 19（local3）*Apache* エラー
  - 20（local4）*etc/opt/apache2*
  - 21（local5）開発者
  - 22（local6）ネットワーク

コールのメディア統計情報ロギング

メディア統計情報を有効にする方法

必要に応じて、Expressway 上でのメディア統計情報の収集を有効にするには、**[メンテナンス（Maintenance）] > [ロギング（Logging）]** に移動し、**[メディア統計情報（Media statistics）]** を *[オン（On）]* に設定します。これにより、システムは各コールのメディア統計情報をロー

カル ハード ディスクの **/mnt/harddisk/log** に記録するようになります。それぞれ 10 MB のファイルが 200 個まで保存されます。200 番目のファイルが一杯になると、最も古いファイルが削除されます。

収集されるメディア統計情報は、転送されたパケット数、損失したパケット数、ジッター、メディア タイプ、コーデック、実際のビットレートなどです。

メディア統計情報も Syslog メッセージとしてパブリッシュされます。メディア統計情報ロギングが有効にされている間、Expressway は機能 18（local2）を使用して、設定したすべてのリモート Syslog サーバに統計情報をパブリッシュします。メッセージのシビラティ（重大度）は *[*情報提供（*Informational*）*]* に設定されますが、メディア統計情報メッセージはシビラティ（重大度）フィルタに関係なく常にパブリッシュされます。

コール詳細レコードのキャプチャ

サービスを有効にする必要がある場合（デフォルトはオフ）、Expressway では、必要に応じて CDR をキャプチャできます。CDR は 7 日の間ローカルに保存され、リモートログを使用している場合は、syslog メッセージとしても公開できます。

CDR の設定方法

Expressway で CDR を設定するには、次の手順を実行します。

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[ロギング オプション（Logging options）]** セクションで、**[コール詳細レコード]** フィールドを必要なオプションに設定します。

- サービスとロギング：CDRs は 7 日間ローカルに保存された後、削除されます。レコードはローカルのイベントログからアクセス可能で、外部ロギングが有効な場合、syslog ホストに INFO メッセージとして送信されます。
- サービスのみ：CDRsは7日間ローカルに保存された後、削除されます。このレコードには、Webユーザインターフェイスからアクセスできません。CDR は REST API を介してのみ読み取り可能です。
- オフ：CDR はローカルではログは記録されません。これがデフォルト設定です。

CDR プロパティ

この表では、CDR に表示されるプロパティを定義します。

フィールド	定義
uuid	CDR エントリの ID。

フィールド	定義
service_uuid	レコードの収集元がプロキシか、Lync 2BUA か、または暗号化 B2BUA かの識別に使用する ID。
active	コールがライブまたは履歴か。
initial_call	コールが複数コンポーネントの場合（B2BUA ホップが含まれる）、B2BUA コールに内部的に関連付けるために使用します。
licensed	コールでライセンスが使用された場合に表示されます。
licensed_as_traversal	コールでトラバーサルライセンスが使用された場合に表示されます。
status	200 OK メッセージは、コールが成功されたことを示します。コールが失敗した場合のエラーメッセージが含まれます。
tag	コール ID。
box_call_serial_number	（B2BUA を介したなど）複数のコールを関連付けするために追加された追加 ID。
start_time	コールの日時。タイムゾーンは、**[システム（System）] > [時刻（Times）] > [タイムゾーン（Time Zone）]** で設定でき、日付形式は YYYY-MM-DD です。
end_time	コールの終了時間。
source_alias	発信者のエイリアス。
destination_alias	呼び出し先のエイリアス。
aside_destination_alias	発信者（または、Lync と相互運用の場合は MS Lync クライアント）のエイリアス。
bside_destination_alias	呼び出し先（または Lync 以外のクライアント）のエイリアス。
aside_request_uri	発信者（または Lync と相互運用の場合は MS Lync クライアント）の要求 URI。
bside_request_uri	呼び出し先（または Lync 以外のクライアント）の要求 URI です。
protocol	コールが SIP <-> SIP, SIP <-> H323, H323 <-> SIP, or H323 <-> H323であったかどうかを示します。

フィールド	定義
protocol_summary	上記のように、コールがマルチコンポーネント、DVO などの追加情報を持つ場合があります。
media_routed	コール中にメディアが送信されたか（NAT/IWF/B2BUA など）が表示されます。
audio	通話が音声専用の通話だったのか示します。
traversal_license_tokens	コールフォーク/ブランチがメディアを使用したかどうかを示します（オーディオは 1 トークン、ビデオは 2 に相当します）。*
non_traversal_license_tokens	コールフォーク/ブランチがメディアを取得する必要がなかったかどうかを示します（オーディオは 1 トークンおよびビデオ 2 に相当します）。*
disconnect_reason	通常のコールティアダウンや他のエラー（つまり最後のステータス）など、コールドロップの理由を示します。
details	メディア統計を含む、コールの詳細を表示します。
last_updated_timestamp	上記のフィールドのいずれかが最後に更新されたとき。

* コールが設定されると、これらのエントリのいずれかがゼロ以外の値になります（応答したフォーク/ブランチについてのみ）。

CDR にアクセスする API

次のセキュアな REST API を使用して、CDR を収集できます。

- get_all_records（最長で 7 日前までのすべてのレコードを返します）。
- get_records_for_interval（指定された時間のレコードを返します）。
- get_records_for_filter（任意の組み合わせを使用して結果をフィルタリングします）。
- get_all_csv_records（最長で 7 日前までのすべてのレコードを csv 形式で返します）。

重要 通話履歴はローカルに 7 日間のみ保存された後、自動的に削除されます。

目的の API にアクセスするには、次の URL を使用します。

https://%3CExpressway_IP%3E/api/external/callusage/%3CAPI%3E

API の例

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_records
- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

入力パラメータ

パラメータ	説明（Description）
fromtime	必須。CDR レコードが必要な期間の開始時刻。 **形式**：*YYYY-MM-DD HH:MI:SS*
totime	必須。CDR レコードが必要な期間の終了時刻。 **形式**：*YYYY-MM-DD HH:MI:SS*

- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

- `http://<Expressway_IP>/api/external/callusage/get_records_for_filter?uuid=<uuid>&src_alias=<src_alias>&dest_alias=<dest_alias>&protocol=<protocol>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_filter?uuid=6e3b5a8a-346c-421b-aa2e-f4409c43a81a
  &src_alias=TC149-057-h323@domain.com&dest_alias=
  TC149-065-h323@domain.com&protocol=H323 <-> H323
  ```

入力パラメータ

パラメータ	説明（Description）
uuid	記録の一意の識別子。
src_alias	コールの発信元。
dest_ alias	コールの宛先ポイント。
protocol	コールに使用されたプロトコル（SIP、H323 など）。

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_csv_records

CDR の例

サンプル CDR

このサンプルの場合、CSV を除くすべての API に適用されます。

[{"initial_call": "false", "protocol": "SIP <-> SIP", "protocol_summary": "", "disconnect_reason": "200 OK", "licensed": "false", "tag": "b8d52a60-16a1-4bdb-be93-f5a675408811", "aside_request_uri": "", "box_call_serial_number": "22cd0e7d-c498-4068-9239-624038fe5130", "source_alias": "sip:10000005@10.196.4.82", "uuid": "800fe013-83f4-4094-a5e6-e2f9489912e2", "last_updated_timestamp": 1444725389, "details": "{\"Call\":{\"SerialNumber\": \"800fe013-83f4-4094-a5e6-e2f9489912e2\",\"BoxSerialNumber\": \"22cd0e7d-c498-4068-9239-624038fe5130\",\"Tag\": \"b8d52a60-16a1-4bdb-be93-f5a675408811\",\"State\": \"Disconnected\",\"StartTime\": \"2015-10-13 01:36:26.485636\",\"InitialCall\": \"False\",\"Licensed\": \"False\",\"LicensedAsTraversal\": \"False\",\"SourceAlias\": \"sip:10000005@10.196.4.82\",\"DestinationAlias\": \"sip:10000010@cucm-82\",\"ToLocalB2BUA\": \"False\",\"Audio\": \"False\",\"License\":{\"Traversal\": \"0\",\"NonTraversal\": \"0\",\"DemotedTraversal\": \"0\",\"CollaborationEdge\": \"0\",\"Cloud\": \"0\"},\"Duration\": \"3\",\"Legs\":[{\"Leg\":{\"Protocol\": \"SIP\",\"SIP\":{\"Address\": \"10.196.4.61:5073\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000005@10.196.4.82\"}}]},\"Targets\":[{\"Target\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000010@10.196.4.116\"}}],\"BandwidthNode\": \"DefaultZone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\": \"OK\"}},{\"Leg\":{\"Protocol\": \"SIP\",\"SIP\":{\"Address\": \"10.196.4.71:7001\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000010@cucm-82\"}}]},\"Source\":{\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"10000005@10.196.4.82\"}}]},\"BandwidthNode\": \"Traversal-zone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\": \"OK\"}}],\"Sessions\":[{\"Session\":{\"Status\": \"Completed\",\"MediaRouted\": \"False\",\"CallRouted\": \"True\",\"Participants\":{\"Leg\": \"1\",\"Leg\": \"2\",\"Incoming\":{\"Leg\": \"1\"},\"Outgoing\":{\"Leg\": \"2\"}}}}],\"EndTime\": \"2015-10-13 01:36:29.745651\"}}", "status": "Disconnected", "destination_alias": "sip:10000010@cucm-82", "licensed_as_traversal": "false", "service_uuid": "e6723fd0-5ca2-11e1-b86c-0800200c9a66", "start_time": "2015-10-13 01:36:26.485636", "traversal_license_tokens": 0, "bside_destination_alias": "", "active": "false", "media_routed": "false", "aside_destination_alias": "", "non_traversal_license_tokens": 0, "bside_request_uri": "", "end_time": "2015-10-13 01:36:29.745651", "audio": "false”}]

csv CDR の例

```
uuid,service_uuid,active,initial_call,licensed,licensed_as_traversal,
status,tag,box_call_serial_number,start_time,end_time,source_alias,
destination_alias,aside_destination_alias,bside_destination_alias,
aside_request_uri,bside_request_uri,protocol_summary,protocol,
media_routed,audio,traversal_license_tokens,non_traversal_license_tokens,
disconnect_reason,details,last_updated_timestamp
```

```
800fe013-83f4-4094-a5e6-e2f9489912e2,e6723fd0-5ca2-11e1-
b86c-0800200c9a66,false,false,false,false,Disconnected,b8d52a60-16a1-
4bdb-be93-f5a675408811,22cd0e7d-c498-4068-9239-624038fe5130,2015-10-
13 01:36:26.485636,2015-10-13
```

01:36:26.485636,2015-10-13 01:36:29.745651,sip:10000005@10.196.4.82,sip:10000010@cucm-82,,,,,,SIP <-> SIP,false,false,0,0,200 OK,"{""Call"":{""SerialNumber"": ""800fe013-83f4-4094-a5e6-e2f9489912e2"",""BoxSerialNumber"": ""22cd0e7d-c498-4068-9239-624038fe5130"",""Tag"": ""b8d52a60-16a1-4bdb-be93-f5a675408811"",""State"": ""Disconnected"",""StartTime"": ""2015-10-13 01:36:26.485636"",""InitialCall"": ""False"",""Licensed"": ""False"",""LicensedAsTraversal"": ""False"",""SourceAlias"": ""sip:10000005@10.196.4.82"",""DestinationAlias"": ""sip:10000010@cucm-82"",""ToLocalB2BUA"": ""False"",""Audio"": ""False"",""License"":{""Traversal"": ""0"",""NonTraversal"": ""0"",""DemotedTraversal"": ""0"",""CollaborationEdge"": ""0"",""Cloud"": ""0""},""Duration"": ""3"",""Legs"":[{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.61:5073"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000005@10.196.4.82""}}]},""Targets"":[{""Target"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@10.196.4.116""}}],""BandwidthNode"": ""DefaultZone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}},{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.71:7001"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@cucm-82""}}]},""Source"":{""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""10000005@10.196.4.82""}}]},""BandwidthNode"": ""Traversal-zone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}}],""Sessions"":[{""Session"":{""Status"": ""Completed"",""MediaRouted"": ""False"",""CallRouted"": ""True"",""Participants"":{""Leg"": ""1"",""Leg"": ""2"",""Incoming"":{""Leg"": ""1""},""Outgoing"":{""Leg"": ""2""}}}}],""EndTime"": ""2015-10-13 01:36:29.745651""}}",1444725389

アラームベースの電子メール通知の設定

Expressway は、アラームのシビラティ（重大度）およびオプションでアラーム ID に基づく電子メールベースの通知をサポートします。設定されている場合、アラームがシステムに生成されると、設定されている宛先アドレスに電子メール通知が送信されます。アラームのシビラティ（重大度）分類ごとに、通知の緊急性を区別するために、異なる電子メール ID を定義できます。同じシビラティ（重大度）のアラームに対して、複数の電子メール ID を設定できます。

X12.6.2 から、特定のアラーム ID の通知を特定の電子メール ID に送信したり、特定のアラーム ID に対する通知を無効にしたりすることもできます。

重要 電子メール ID の最大許容長は 256 文字です。

この機能は、Kari の法律を実装したい米国を拠点とするお客様にもご利用いただけます。Expressway を経由して直接 9-1-1 をダイヤルする基準を満たす 9-1-1 コールが行われた場合、シビラティ（重大度）のアラーム緊急が生成され、(設定されている場合)、シビラティ（重大度）のアラーム緊急用に設定された電子メール ID に通知が送信されます。

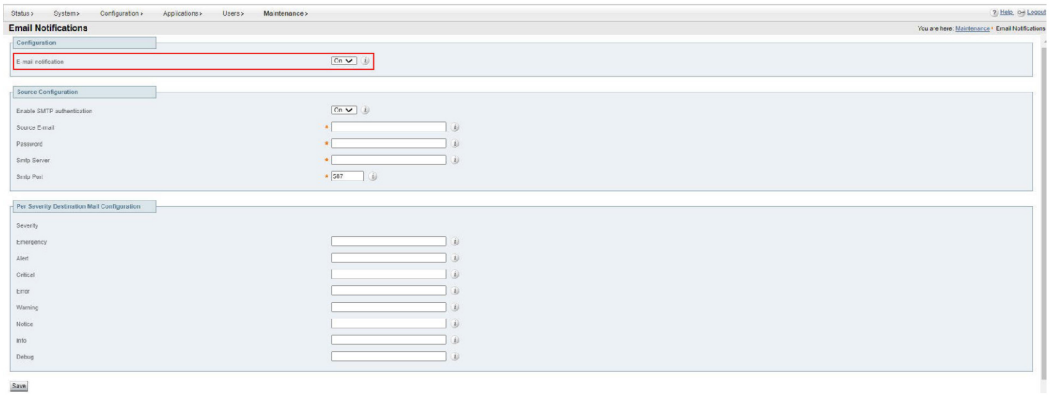
はじめる前に

- 電子メールを送信するための接続を確立するために、SMTP サーバの詳細を提供する必要があります。
- Expressway は、SMTP サーバとの TLS 接続のみをサポートしています。
- SMTP サーバは、Expressway から直接、または SMTP プロキシを使用して到達できる必要があります。SMTP 用の HTTP プロキシの使用はサポートされていません。
- 送信元の電子メールとパスワードは、SMTP サーバで検証してから、メールを送信します。
- X12.7 から、Expressway では、TLS 1.2 証明書ベースの検証を使用するために SMTP サービスが必要です。
  - クライアントは SMTP サーバー証明書を検証するため、その IP アドレスや完全修飾ドメイン名（FQDN）が証明書の共通名（CN）/サブジェクト代替名（SAN）に含まれている必要があります。
  - SMTP サーバー証明書の発行者は、Expressway の信頼できる認証局（CA）の証明書リストにインポートする必要があります（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA Certificate）]**）。

アラームベースの電子メール通知を設定をするプロセス

ステップ 1 **[メンテナンス（Maintenance）]** > **[電子メール通知（Email Notifications）]**に移動します。

ステップ 2 **[電子メール通知（Email Notifications）]** ドロップダウンリストで、*[オン（On）]* を選択します。



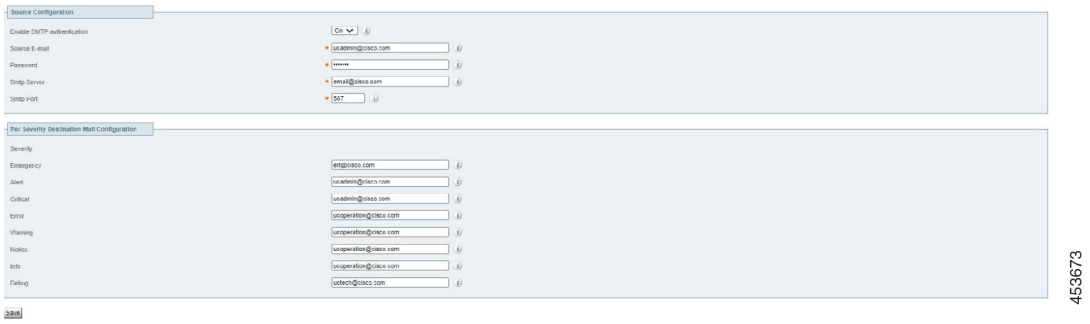
ステップ 3 **[送信元の設定（Source Configuration）]** セクションに次の情報を入力します。

- **SMTP 認証の有効化（Enable SMTP authentication）**：SMTP サーバー認証はデフォルトで有効になっています（*[オン（On）]* 状態）。ドロップダウンリストでは、*[オン（On）]* 状態と *[オフ（Off）]* 状

態を切り替えることができます。ユーザーのSMTPサーバーが認証を必要としない場合にのみ、*[*オフ（*Off*）*]* にする必要があります。ほとんどのユーザーにはこれが必要です。

- 設定された宛先アドレスに通知が送信される送信元のメールアドレス。
- 電子メール通知の送信に使用される SMTP サーバの IP アドレスまたは FQDN。
- **[シビラティ（重大度）ごとの宛先メール構成]** セクションで、特定のシビラティ（重大度）のアラームの通知を受信する電子メールアドレスを入力します。
- [保存（Save）] をクリックします。

図 *1:* 電子メール通知の設定例



通知のカスタマイズ方法 - 無効化または電子メールアドレスへ送信

必要に応じて、このプロセスを使用して、特定のアラーム ID の通知を特定の電子メールアドレスに送信したり、特定のアラーム ID に対する通知を無効にしたりすることができます。たとえば、指名された個人にしきい値警告アラームを送信したり、不要なアラームによる通知を停止したりすることができます。

ステップ 1 **「電子メール通知」** ページの **「カスタム通知」** セクションに移動します。ここで、既存のカスタム通知を表示、編集、および削除し、新しい通知を追加できます。

ステップ 2 カスタマイズされた通知を作成するには

1. [追加（Add）] をクリックします。
2. 使用するアラーム ID を選択します。
3. **[通知]** ドロップダウンリストで、選択したアラームの電子メール通知先を定義する場合は *[*カスタム*]* を選択し、このアラームに対して電子メールを送信しない場合は *[*無効にする*]* を選択します。
4. [カスタム] を選択した場合は、**[電子メール]** フィールドに、選択したアラーム通知の送信先である通知先の電子メールアドレス を入力します。

5. [保存（Save）] をクリックします。
6. アラーム通知が意図した通り動作することをテストするには、次の作業を実行します。
   1. **[アラームの選択]** ドロップダウンから、テストするアラームを選択します。
   2. **[今すぐテスト（Test Now）]** ボタンをクリックします。
   3. テストから受信した電子メール通知が期待通りか確認します。

電子メール通知の削減

この改善の目的は、何らかの理由で短期間に複数のアラームが発生した場合に、管理者を電子メールでスパミングしないようにすることです。

X14.2 以降は、1 時間以内に同じアラームが 2 回以上発生した場合、電子メールは 1 回だけ送信されます。同じアラームが止み、再び発生した場合は、経過時間に関係なく電子メールが送信されます。当然、これは、管理者がデバイスで電子メール通知を受信するように構成している場合にのみ適用されます。

Note 過去1時間以内に特定のアラームに関する電子メールがすでに送信されている場合、システムは電子メール通知を繰り返し送信しません。

次に例を示します。

1. 例 1
   a. ID 15000 のアラームは 14:00 に発生します。
   b. 電子メール通知を構成すると、ID 15000 のアラームに電子メールが送信されます。
   c. 同じアラーム（ID 15000）が 14:55 に発生します。1 時間が経過していないため、電子メール通知は送信されません。ただし、同じアラームが 15:01 に発生した場合は、電子メール通知が送信されます。
2. 例 2
   a. ID 15000 のアラームは 14:00 に発生します。
   b. 電子メール通知を構成すると、ID 15000 のアラームに電子メールが送信されます。
   c. 同じアラームが 14:05 に発生します。
   d. ID 15000 のアラームが 14:10 に再度発生します。
   e. ID 15000 のアラームの電子メール通知が再送信されます。

システム メトリック コレクション

システムメトリックの収集は、システムパフォーマンスに関する統計情報をパブリッシュする機能で、パフォーマンスをリモートからモニタできるようにします。Expressway は、ハードウェア、OS、およびアプリケーションのパフォーマンスに関する統計情報を収集し、データを集約するリモートホスト（通常はデータ分析サーバ）にそれらの統計情報をパブリッシュします。この機能は Web インターフェイスまたはコマンドラインで設定できます。

（注） 1 つのピアからの設定はクラスタ全体に適用されます。クラスタをモニタする場合は、プライマリピアに System Metrics Collection を設定することをお勧めします。

リモートサーバの設定も必要です。収集されたスレッドはサーバ上で実行されている必要があります。収集されたネットワークプラグインは、クライアントに見えるアドレスをリッスンするように設定されています。設定の詳細はモニタリング環境によって異なり、このガイドの範囲を超えています。

収集したデータの使用方法

Expresswayから収集されたデータに基づいて、グラフを生成し、統計を集約し、パフォーマンスを解析するために、Circonus および Graphite などのツールを使用できます。また、トレンドを表示し、潜在的な問題を予想する場合にも使用できます。表示できるメトリックには、次のものがあります。

- ゾーン単位およびシステム別のアクティブコール
- キープロセスメトリック：キープロセスのシステム CPU、ユーザ CPU、およびメモリ使用量
- アラーム

システムメトリック収集（収集済み）の構成方法

Expressway を設定する

必要に応じて、Web ユーザインターフェイスから Expressway を設定し、統計を収集、指定されたサーバに公開するには、次の手順を使用します。

（注） CLIから収集をオンにするには、システムメトリックサーバーのIPアドレスが必要です（Web ユーザーインターフェイスと同様の動作）。

ステップ 1 Expressway にログインし、**[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[システム メトリックの収集（System Metrics Collection）]** を *[オン（On）]* に切り替えます。

ステップ 3 [収集サーバのアドレス（Collection server address）] に入力します。

IP アドレス、ホスト名、または FQDN を使用してリモートサーバを特定できます。

ステップ 4 必要に応じて、デフォルトの **収集サーバポート**（リスニングポート）を変更します（収集サーバがデフォルト以外のポートでリッスンしている場合）。

ステップ 5 必要に応じて、デフォルトの**収集間隔**を変更します（ポリシーでデフォルトの間隔の 60 秒よりも細かく調整されたメトリックが必要な場合）。

ステップ 6 [保存（Save）] をクリックします。

収集したものを構成する CLI コマンドの例

CLI を使用する場合は、関連するコマンドの例を以下となります。

表 *2 :* 収集を設定する *CLI* コマンド

コマンドの機能	コマンド例
メトリック収集のオンとオフの切り替え	**xconfig log SystemMetrics mode: on**
サーバアドレスの指定	**xconfig log SystemMetrics network address: address**
リスニングポートの指定	**xconfig log SystemMetrics network port: 25826**
収集間隔の指定	**xconfig log SystemMetrics interval: 60**
システムメトリック設定の読み取り	**xstatus SystemMetrics**

リモートサーバを設定する

使用している環境でのデータ分析に選択するサーバの使用と設定は、このマニュアルでは扱いません。回収された情報を処理できるアプリケーションの一例です。分析ツールは、collectd デーモンからのデータの受信をサポートする必要があります。このデーモンは Expressway で実行され、collectd ネットワーク プラグインを使用してメトリックを分析サーバにプッシュします。

ネットワーク プラグインは、データのカプセル化のための収集したバイナリプロトコルを実装します。分析サーバは、このデータを解析し、提示できる必要があります。分析サーバには、collectd ソフトウェアまたは代替ソフトウェアに基づいてデータの収集方法や表示方法を設定するための独自の UI が備わっている可能性があります。

分析サーバで collectd を使用している場合は 、*collectd.conf* ファイルを変更 して、サーバが次の条件を実行します。

- 収集されたクライアント（Expresswayなど）からデータをリッスンします。ネットワークプラグインを有効にして、サーバの IP アドレスでリッスンブロックを設定する必要があります。次に例を示します。

```
<Plugin "network">
                Listen "198.51.100.15"
        </Plugin>
```

- 受信したデータを人が読み取り可能な形式（CSV ファイルなど）に格納します。csv プラグインを有効にして、ファイルの書き込み場所を知る必要があります。次に例を示します。

```
<Plugin "csv">
                 DataDir "/var/lib/collectd/csv"
                 StoreRates true
        </Plugin>
```

詳細情報

- https://collectd.org/wiki/index.php/Networking_introduction
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_network
- https://collectd.org/wiki/index.php/Binary_protocol
- https://collectd.org/wiki/index.php/Plugin:CSV
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_csv

トラブルシューティング

Expressway がデータを送信するかどうかを確認するには、Expressway から TCP ダンプを設定し、データ分析サーバのアドレスに送信されたパケットを確認します。**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [診断のログ（Diagnostics logging）]** に移動し、**ロギング中に tcpdump を取得（Take tcpdump while logging）** チェックボックスをオンにし、ロギングを開始します。

Expressway から収集されたメトリック

次のハードウェア統計情報がモニタされます。

- aggregation-cpu-sum
- aggregation-cpu-average
- システム内の各コアのコア単位の CPU 使用状況
- df
- ディスク
- 負荷
- protocols-Tcp

- protocols-Udp
- swap
- ユーザ
- メモリ
- アップタイム
- プロセス

次のアプリケーションデータは、collectd のカスタム exec-app プラグインによってモニタされます。

- `gauge-active_alarms` は、この Expressway 上のアクティブなアラームの数です。
- `gauge-active_calls` は、この Expressway によって処理中のコールの数です。
- `gauge-<service name>`は、各システムサービスのステータスです。
- `gauge-<zone name>_ActiveCalls`は、名前付きゾーン内のアクティブコールをカウントします。
- `gauge-<zone name>_BandwidthAllocated`は、指定されたゾーンに割り当てられた合計帯域幅を測定します。
- `gauge-<zone name>_BandwidthLimit`

これらのメトリックのそれぞれが自由形式のデータを許可する collectd GAUGE データソースタイプを使用します。収集サーバでは、たとえば、*collectdHostnamecollectd.exec-app.gauge-active_calls* のように、完全な collectd 値の名前が表示されます。

（注） ゾーン名はユーザが設定できる構成のため、収集されたメトリックの名前スキーマと競合している可能性があります。収集サーバがスキーマを適用している場合、一部のゾーンからのメトリックが受け付けられない可能性があります。

収集サーバに送信されるデータ

ネットワークプラグインは収集されたバイナリプロトコルを使用して、モニタ対象のハードウェアリソースやソフトウェアプロセスを表す数字、文字列、および値データをカプセル化します。ネットワークプラグインは、デフォルトで UDP 25826 を使用して、分析サーバにメトリックのデータパケットを間隔ごとに 1 回プッシュします。分析サーバはデータを解析し、人間が判読できる形式で表示します。

分析サーバが収集されたネットワークプラグインと csv プラグインを使用している場合、メトリック名とタイムスタンプを使用してファイル名を作成し、メトリックは小規模な CSV ファイルとして保存されます。たとえば、*gauge-H323-2015-05-21*

収集されたプラグイン

収集されたこれらのプラグインは、Expressway に実装されます。

プラグイン名	説明（Description）
アグリゲーション	CPU 値をカウンタの `aggregation_cpu_sum` と `aggregation_cpu_average` に集約します。
CPU	プロセッサ情報raw 情報が `aggregation_cpu_average` と `aggregation_cpu_sum` に集約されます。
DF	ファイル システム情報。collectd Wiki の DF の説明を参照してください。
ディスク	ハードディスクのパフォーマンス。collectd Wiki のディスクの説明を参照してください。

プラグイン名	説明（**Description**）
Exec-app	コール、アラーム、ゾーン、およびサービスに関する特定の Expressway 情報を返すカスタマイズされた **exec** バージョン • gauge-active_alarms → Expressway でアクティブなアラーム数 • gauge-active_calls → Expressway が処理処理したアクティブ通話数 • gauge-B2BUA → B2BUA サービスのステータス • gauge-callusagemanager → CDR に使用されるサービスのステータス • gauge-<zone>_ActiveCalls → 指定されたゾーン内のアクティブな通話をカウント • gauge-<zone>_BandwidthAllocated → 指定ゾーンに割り当てられたそう帯域幅を測定 • gauge-c_mgmt → ManagementConnector サービス • gauge-collectd → Collectd サービスのステータス • gauge-edgeconfigprovisioning → MRA で使用されるプロビジョニングサービスのステータス • gauge-fail2ban → 自動保護機能で使用される fail2ban サービスのステータス • gauge-findmed → TMS プロビジョニングで使用される FindMe サービスのステータス

プラグイン名	説明（Description）
Exec-app	• gauge-H323 → H.323 サービスハンドラのステータス • gauge-http → HTTP 要求を HTTPS にリダイレクトするステータス • gauge-https → Web インターフェイスの有効化/無効化 • gauge-importcontrol → TMS プロビジョニングで使用されるサービスのステータス • gauge-jabberd → XMPP で使用されるサービスのステータス • gauge-phonebookserver → Phonebook サービスのステータス • gauge-portforwarding →トラフィックサーバー（ATS）で使用されるサービスのステータス • gauge-provisioningd → TMS プロビジョニングで使用されるサービスのステータス • gauge-provisioningserver → プロビジョニングサーバーのサービスステータス • gauge-proxy-registrationd → Exp-E のプロキシ登録のカウンタ • gauge-restmanager → RESTAPI サービスのステータス • gauge-samlverifier → SAML SSO で使用されるサービスのステータス • gauge-SIP → SIP サービスハンドラのステータス • gauge-snmpd → SNMP サービスのステータス • gauge-sshd → SSH サービスのステータス

プラグイン名	説明（Description）
Exec-app	• gauge-sshdpfwd → MRA/WebRTC などで使用される SSH PortForwarding サービスのステータス • gauge-sslh → WebRTC および TURN で使用されるサービスのステータス • gauge-trafficserver →MRA/WebRTC などに使用される ATS サービスのステータス • gauge-winbindd → 内部 Expressway サービス、サービスのステータス
負荷	タスクキューに基づくシステム負荷。
メモリ	メモリの統計情報。
ネットワーク	リモートアドレスへのパブリッシュを可能にします。このプラグインは、データのカプセル化のための collectd バイナリプロトコルを実装します。リモートサーバには適切な解析ツールが必要です。
プロトコル	Expressway で使用されるプロトコルの設定可能なサブセット。

プラグイン名	説明（Description）
プロセス	システムプロセスをカウントし、状態（実行中、スリープ中、ゾンビなど）ごとにグループ化します。また、特定のプロセスの詳細な統計情報を収集します。プラグインは次のプロセスを詳しくモニタします。 • app → メイン APP プロセスのステータス • bramble → 廃止、プレゼンス通知に使用 • credentialmanagerservermain → 認証目的に使用されるプロセスのステータス • cvs_main → 証明書検証プロセスのステータス • erlang-beam → 内部 CDB プロセスのステータス • erlang-epmd → 内部 CDB プロセスのステータス • httpd → HTTP デーモンプロセスのステータス

プラグイン名	説明（**Description**）
プロセス	• httpserver → HTTP サーバープロセスのステップ • ivy → 内部 B2BUA プロセスのステータス • licensemanagerservermain → ライセンスプロセスのステータス • managementconnectormain → Management Connector プロセスのステータス • managementframework → 内部プロセスのステータス • openssl2nss → SSL プロセスのステータス。 • policyservermain → コールルーティングなどに使用されるポリシーサービスのステータス • sshdpfwd → SSH ポート転送プロセスのステータス（MRA、WebRTC で使用） • syslog-ng → Syslog プロセスのステータス • traffic_server → MRA、WebRTC で使用される ATS プロセスのステータス • XCP → JabberD を使用した内部プロセスのステータス

プラグイン名	説明（Description）
Statsd	特定の Expressway 情報を返すカスタマイズされたバージョン。たとえば、ICE 使用法です。 • gauge-ICEPassthroughMetrics.b2buacalls → B2BUA 通話に接続 • gauge-ICEPassthroughMetrics.candidatesofferedmissingiceconfig → B2BUA 通話は接続されていますが、入力/出力ゾーンが ICE パススルー用に正しく設定されていません。1 つまたは両方のエンドポイントが ICE を提供する場合は、調査する構成の問題がある可能性があることを示すメトリックをペグします。 • gauge-ICEPassthroughMetrics.failedicenegotiationcalls → Expressway は ICE パススルー用に構成されており、エンドポイントは ICE をネゴシエートしようとしていたが、一方または両方が Remote Candidate を送信できませんでした。 • gauge-ICEPassthroughMetrics.hosthostcalls → 両側にリモート候補があり、両側に Local Candidate タイプが選択されています。これは ICE パススルー通話、Host Candidate と Host Candidate です。 • gauge-ICEPassthroughMetrics.hostrelaycalls → 両側にリモート候補があり、両側に Local Candidate 候補タイプが選択されています。これは ICE パススルー通話、Host Candidate と Relay Candidate です。 • gauge-ICEPassthroughMetrics.hostsrvrflxcalls → 両側にリモート候補があり、両側に Local Candidate タイプが選択されています。これは ICE パススルー通話、Host Candidate と Server Relay Candidate です。 • gauge-ICEPassthroughMetrics.icecalls → 両側にリモート候補があり、両側に Local Candidate タイプが選択されています。これは ICE パススルー通話です。 • gauge-ICEPassthroughMetrics.icecandidatecalls → 一方または両方が ICE 候補を提示しました。 • gauge-ICEPassthroughMetrics.iceconfiguredcalls → B2BUA 通話が接続され、両側が ICE パススルー用に適切に構成されました。 • gauge-ICEPassthroughMetrics.noicecandidatesoffered → どちらの側も ICE 候補を提示しませんでした。

プラグイン名	説明（Description）
Statsd	• gauge-ICEPassthroughMetrics.onepartyicecandidatecalls →一方または両方が ICE candidate を提示しました。 • gauge-ICEPassthroughMetrics.relayrelaycalls → 両側にリモート候補があり、両側に Local Candidate タイプが選択されています。これは ICE パススルー通話、Relay Candidate と Relay Candidate です。 • gauge-ICEPassthroughMetrics.srvrflxrelaycalls → 両側にリモート候補があり、両側にローカル Candidateタイプが選択されています。これは ICE パススルー通話、Server Reflexive Candidate と Relay Candidate です。 • gauge-ICEPassthroughMetrics.srvrflxsrvrflxcalls → 両側にリモート候補があり、両側に Local Candidate タイプが選択されています。これは ICE パススルー通話で、Server Reflexive Candidate と Server Reflexive Candidate です。
Swap	ディスクに書き込まれるシステムメモリの量。
アップタイム	システムの稼働時間を追跡し、平均実行時間や特定の期間の最大アップタイムなどのカウンタを提供します。collectd Wiki のアップタイムの説明を参照してください。
ユーザ	現在ログインしているユーザの数。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。